IMPLEMENTACIÓN DE SERVICIOS DE GESTIÓN DE INFRAESTRUCTURA IT BAJO PLATAFORMAS GNU/LINUX ZENTYAL SERVER COMO SISTEMA OPERATIVO

Edilberto Robles Cruz
e-mail: eroblescr@unadvirtual.edu.co
Kenned Jeffrey Guevara Muñoz
e-mail: kenned_19101@unadvirtual.edu.co
Wilson Ernesto Faura Estupiñán
e-mail: wefaurae@unadvirtual.edu.co
Hayder Manuel Mosquera Tordecilla
e-mail: hmmosquerat@unadvirtual.edu.co
Diego Andrés Peñas Cárdenas
e-mail: dapenacar@unadvirtual.edu.co

RESUMEN: *De acuerdo con el planteamiento y contextualización del problema a resolver que son las problemáticas de migración de sus sistemas operativos, servicios y puesta en marcha de los sistemas de seguridad de la infraestructura de red, donde se pretende dar solución con la implementación de servicios de gestión de infraestructura IT de mayor nivel para Intranet y Extranet en las compañías y/o instituciones complejas bajo plataformas GNU/LINUX Zentyal server como sistema operativo con la instalación, configuración e implementación de los siguientes servicios de gestión de infraestructura: DHCP server, DNS server, controlador de dominio, proxy no transparente, cortafuegos, file server, print server, VPN, lo anterior se administra desde la dashboard del server Zentyal que es una interfax tipo web, el cual permite interactuar y administrar todos los servicios anteriormente mencionados, logrando realizar una ejecución y parametrización de todos estos bajo plataformas GNU/LINUX y su comprobación de la aplicabilidad desde una estación de trabajo GNU/Linux Ubuntu Desktop.*

PALABRAS CLAVE: Controlador de Dominio, Cortafuegos, File server, Print Server, Proxy no transparente, VPN, Zentyal.

1. INTRODUCCIÓN

El presente *trabajo* (paso 8) tiene como propósito de realizar una implementación de servicios de gestión de infraestructura IT de alto nivel para Intranet y Extranet con la utilización de plataformas GNU/LINUX para realizar todo lo que abarca con la solución de necesidades específicas con son servicios de gestión de infraestructura IT, donde se configura y administra los servicios de DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server y Print Server, File Server y Print Server, para dar respuesta a la necesidad mencionada, se aplica el uso de sistema operativo Zentyal Server 5.0. que es una solución integral basada en GNU/LINUX y administrada desde la dashboard tipo web, este servidor que brinda un innumerable servicio de administración y/o gestión de red para así implementar un mayor nivel y control de la infraestructura tecnológica de una compañía y/o institución compleja, permitiendo planear, estructurar, implementar y administrar los diferentes servicios y plataformas con parámetros reglas y permisos de conectividad de la red, de seguridad, de control, de acceso a la información, así poder establecer una infraestructura que brinde disponibilidad, integridad y confidencialidad de la información.

2. INSTALACIÓN DE ZENTYAL SERVER

2.1. REQUISITOS MÍNIMOS:

Para la implementación de Zentyal Server y que pueda funcionar correctamente se requiere unos mínimos requisitos de máquina, así:

Tare

- ✓ Tarjeta de RAM de 2GB.
- ✓ Disco duro de 8GB.
- ✓ Procesador de doble núcleo.
- ✓ Tarjetas de red 2 (para WAN y LAN).

Estos requisitos como mínimos deben tenerse en cuenta a la hora de crear la maquina virtual para el servidor.

2.2. DESCARGA DE ZENTYAL:

Se realiza la descarga de la distribución de Zentyal Server 5.0.1. de GNU/ Linux en archivo de tipo .ISO, desde la página oficial de Zentyal http://download.zentyal.com/, para ser montada en la unidad de CD/DVD de la maquina virtual.

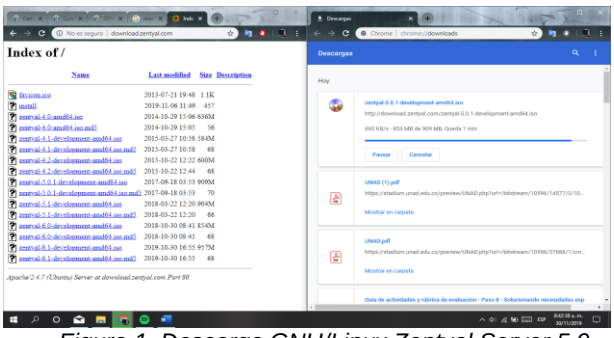


Figura 1. Descarga GNU/Linux Zentyal Server 5.0 – Fuente propia

2.3. INSTALACIÓN DE ZENTYAL

Se inicia la máquina virtual con la imagen .ISO montada para su instalación:

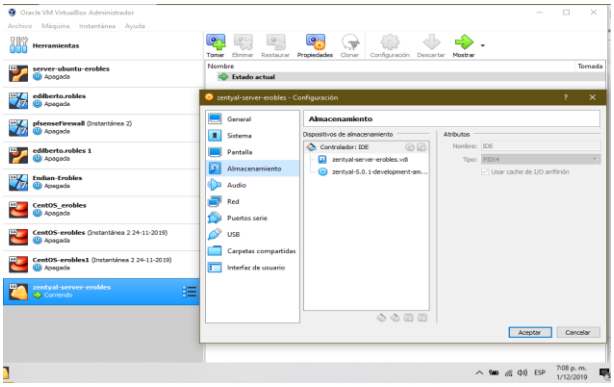


Figura 2. Inicio de máquina virtual para Zentyal Server 5.0. – Fuente propia.

Después de iniciar la maquina virtual con la imagen .ISO montada se da el inicio de la instalación del Zentyal server:

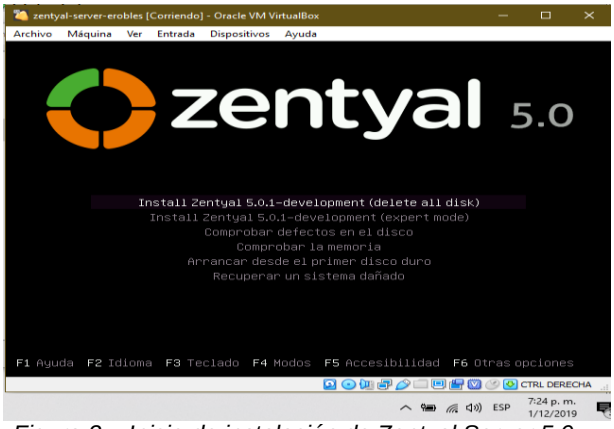


Figura 3 – Inicio de instalación de Zentyal Server 5.0. – Fuente propia

Configuramos el nombre de la máquina, usuario, horario y fecha e inicia la instalación:

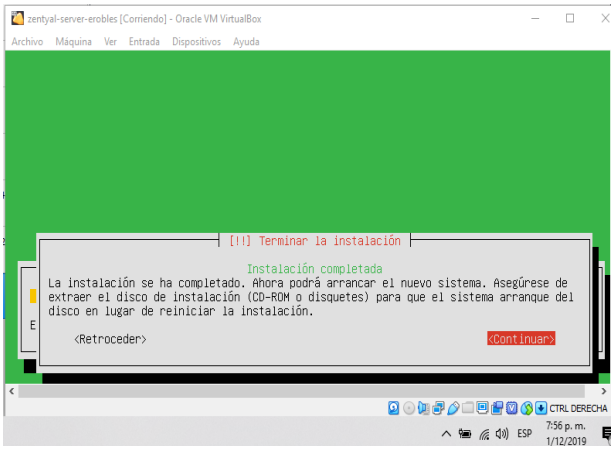


Figura 4 – Instalación básica de Zentyal Server exitosa– Fuente propia

2.4. INGRESO Y CONFIGURACIÓN DE ZENTYAL

Ya finalizado la instalación se reinicia el server:

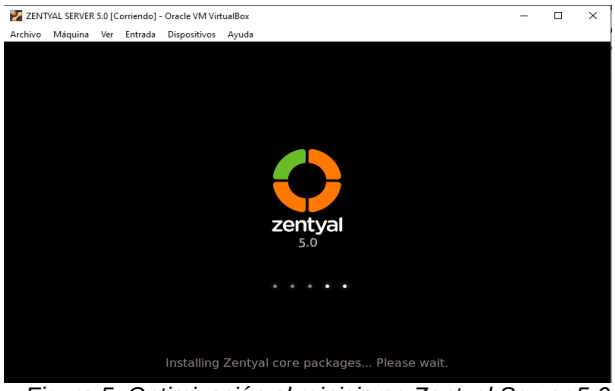


Figura 5. Optimización al reiniciarse Zentyal Server 5.0. – Fuente propia.

Después de reiniciar el server arroja a una página no segura el cual es https://localhost:8443 aceptando el riesgo se ingresa con el usuario y contraseñas creada en su instalación y ya se está en el servidor zentyal para dar inicio a sus configuraciones básicas

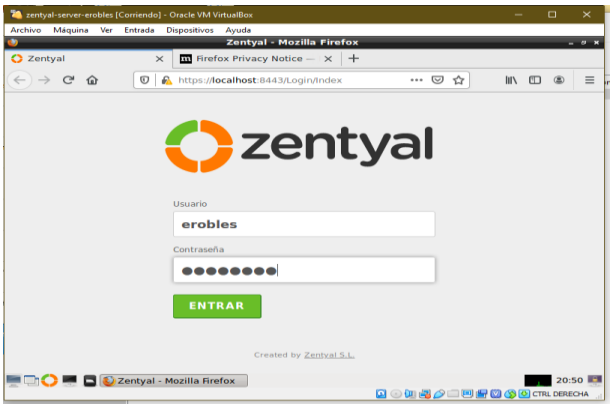


Figura 06 – Ingreso de la Dashboard del server de Zentyal – Fuente propia.

A continuación, se procede a la configuración básica desde la dashboard.

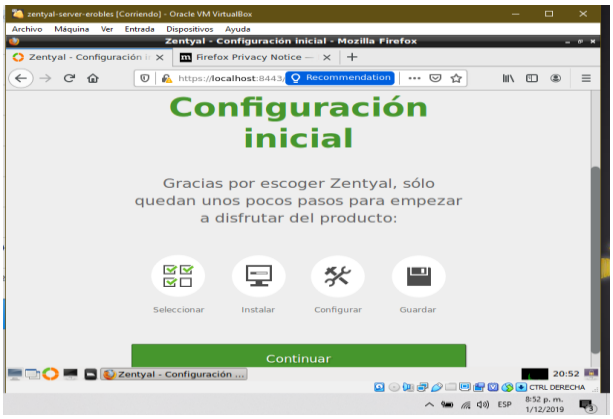


Figura 7 –Configuración básica de la Dashboard del server de Zentyal – Fuente propia

Se realiza la selección e instalación de los servicios y/o paquetes de acuerdo con las funcionalidades que se requiere o va a realizar el servidor Zentyal.

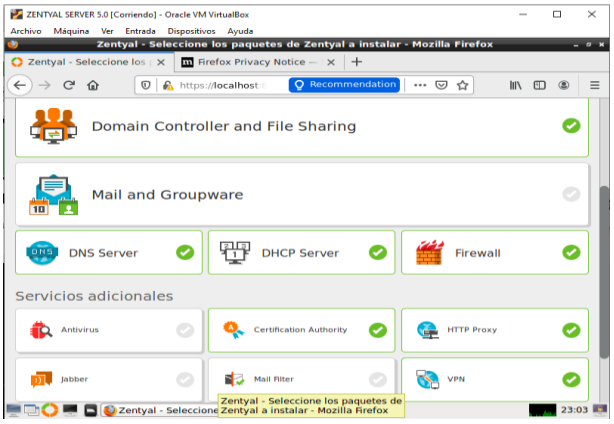


Figura 8 – Roles y/o servicios Zentyal – Fuente propia

Configuramos las interfaces de red (WAN y LAN) de acuerdo con los roles y/o servicios que va a realizar el Servidor de Zentyal:

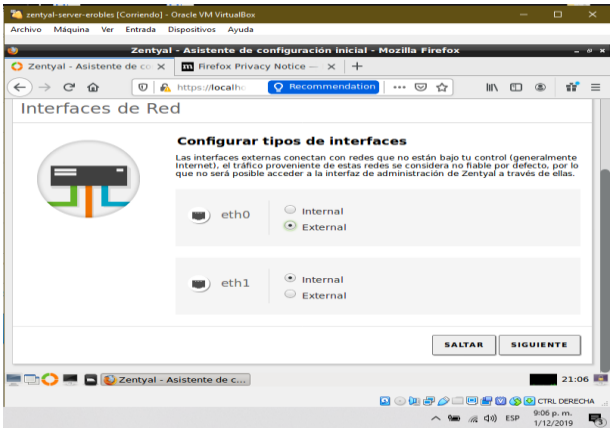


Figura 9 – Configuración de interfaces de red del server Zentyal – Fuente propia

Después de culminar la configuración inicial, arroja la información básica del server y toda la información para su administración.

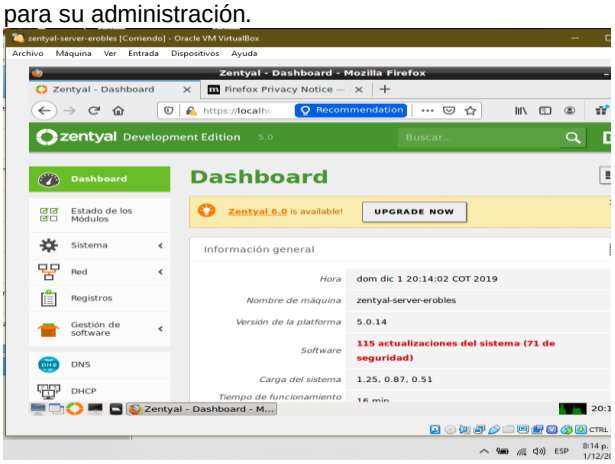


Figura 10 – Administración desde la dashboard del server de Zentyal – Fuente propia

3. IMPLEMENTACIÓN DE SERVICIOS DE GESTIÓN DE INFRAESTRUCTURA IT BAJO ZENTYAL SERVER.

Después de haber culminado ´la instalación y configuración de Zentyal Server como sistema operativo base para disponer de los servicios de Infraestructura IT, se procede a la implementación de estos últimos de acuerdo con cinco (05) temáticas principales, como muestra la siguiente tabla:

Tabla 1. Temáticas a realizar.

No. Temática	Descripción Temática
1	DHCP Server, DNS Server y Controlador de Dominio
2	Proxy no transparente
3	Cortafuegos
4	File Server y Print Server
5	VPN

3.1. TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux Ubuntu Desktop a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.

3.1.1. CONFIGURACIÓN SERVIDOR DHCP

Se descargar el módulo DHCP Server, esto lo hacemos desde la interfaz de zentyal, en el menú de la parte izquierda se sigue la ruta de gestión de software, componentes de Zentyal, seleccionando DHCP Server, luego clic en instalar.

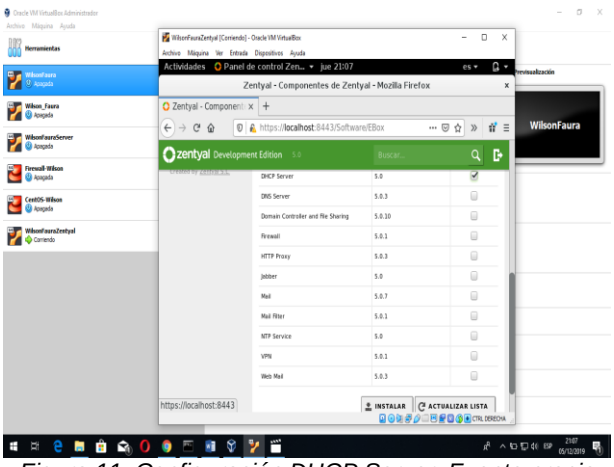


Figura 11. Configuración DHCP Server. Fuente propia

Antes de iniciar la instalación se mostrará un resumen de los paquetes a instalar, además del paquete DHCP, también se instalará el paquete firewall, simplemente se da clic en continuar para seguir con el proceso.

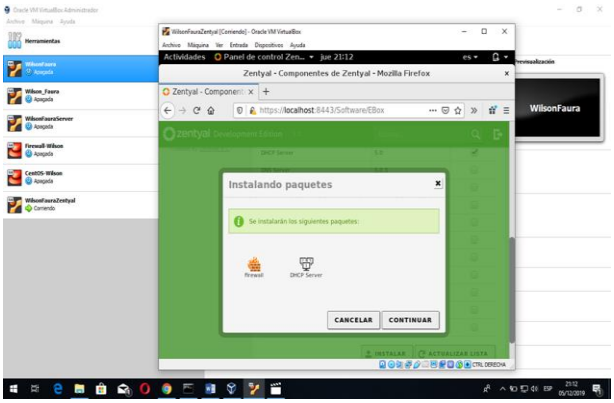


Figura 12. Configuración DHCP Server – *Fuente propia.*

Una vez hecho esto comenzará la instalación de los paquetes, ahora solo esperamos a que se complete el proceso. Por último, nos aparece un mensaje con la confirmación de la instalación, damos en ok.

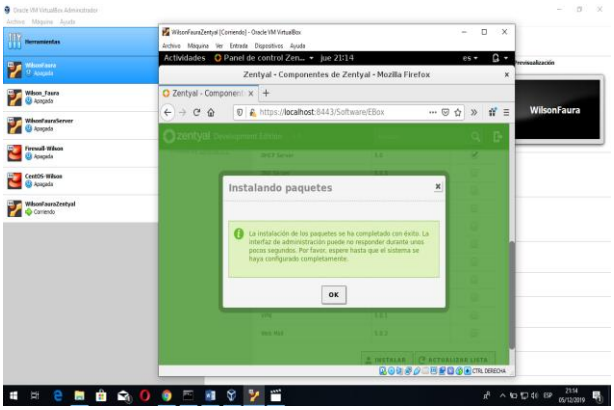


Figura 13. Configuración DHCP Server – Fuente propia.

Una vez descargado el módulo de DHCP aparece en el menú, se procede a seleccionarlo y una vez adentro se puede ver que se encuentra deshabilitado y no posee ningún rango de direcciones configuradas, se hace clic en configuración.

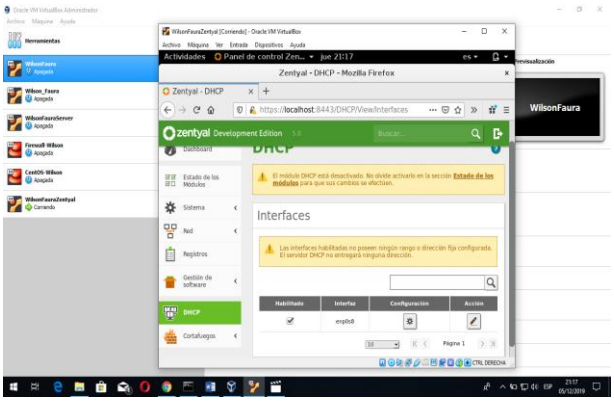


Figura 14. Configuración DHCP Server – Fuente propia.

Ya en la interfaz de configuración se deja como puerta de enlace predeterminada la que aparece por defecto (Zentyal), y como servidores de nombres se pone los de google por el momento tal como lo muestra la figura. Luego se guarda los cambios.

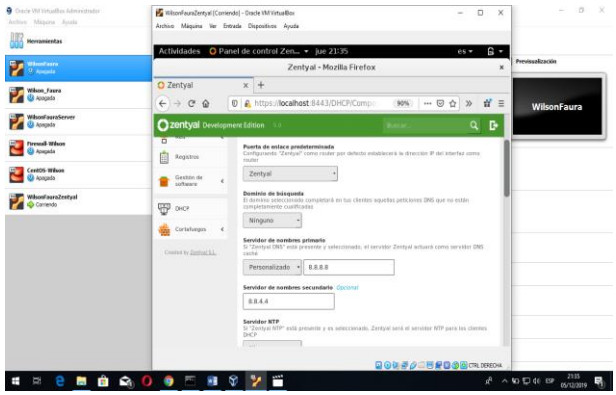


Figura 15. Configuración DHCP Server – Fuente propia.

Nos desplazamos más abajo en la misma interfaz y observamos información sobre los rangos DHCP, podemos ver la dirección IP de la interfaz, la subred y el rango disponible, ahora creamos un nuevo rango con el nombre y las direcciones disponibles. Luego guardamos.

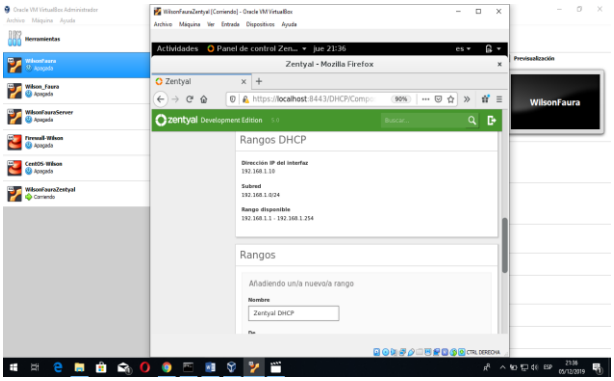


Figura 16. Configuración DHCP Server – Fuente propia.

Como podemos ver en esta pantalla ya se ha creado el nuevo rango de direcciones con el nombre Zentyal DHCP entre las direcciones 192.168.1.20 hasta 192.168.1.25.

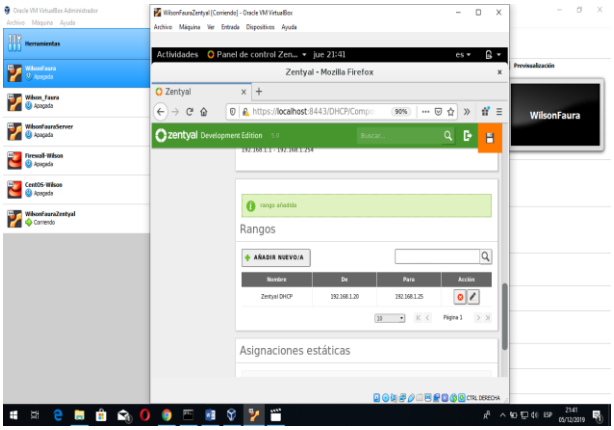


Figura 17. Configuración DHCP Server – Fuente propia.

Luego se configura un cliente previamente instalado dentro de la misma red, seleccionamos el método de direccionamiento IPv4 de forma automática para que el servidor Zentyal sea el que asigne esa IP gracias a la configuración realizada. Luego reiniciamos.

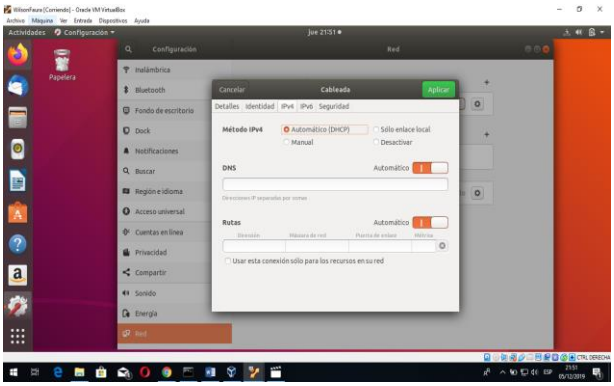


Figura 18. Configuración DHCP Server – Fuente propia.

Como se puede ver en la siguiente figura el servicio DHCP de Zentyal está funcionando correctamente, pues la dirección IP asignada al cliente Ubuntu wilsonfaura es la 192.168.1.20 y la esta asignando el servidor DHCP.

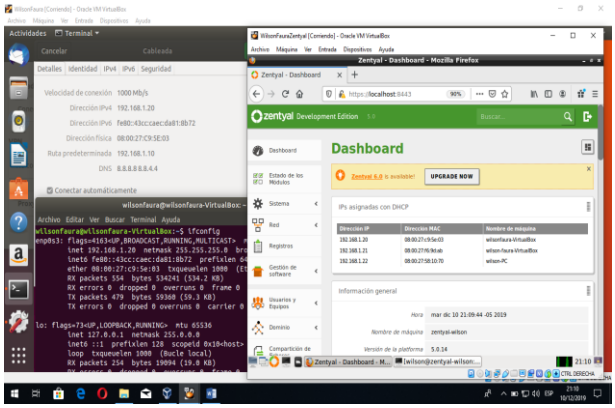


Figura 19. Configuración DHCP Server – Fuente propia

3.1.2. CONFIGURACIÓN SERVIDOR DNS

Ahora se descarga el módulo DNS Server, esto se hace desde la interfaz de zentyal, en el menú de la parte izquierda siguiendo la ruta gestión de software, componentes de Zentyal, seleccionando DNS Server, luego se da clic en instalar.

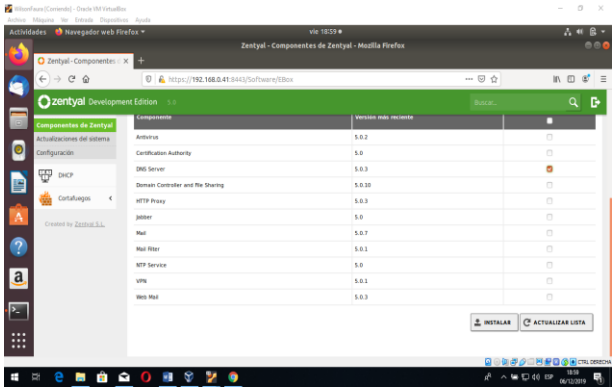


Figura 20. Configuración DNS Server – Fuente propia

Una vez descargado el módulo de DNS aparece en el menú, lo seleccionamos y una vez adentro podemos ver que se encuentra desactivado, en esta parte se configura y habilita el cache de DNS transparente, direccionadores y dominios.

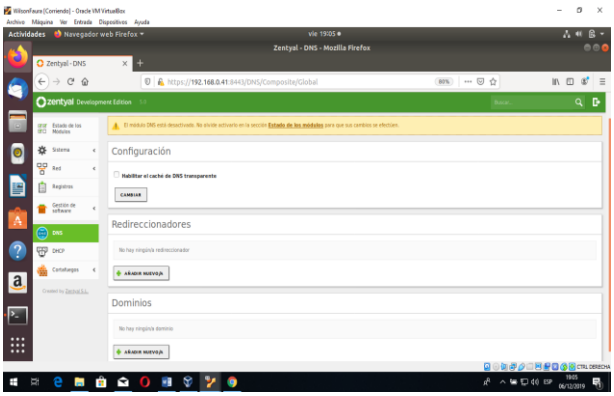


Figura 21. Configuración DNS Server – Fuente propia

Como ejemplo podemos crear un nuevo dominio, damos clic sobre añadir nuevo dominio y creamos el dominio zentyal.com. En esta parte podemos asignar direcciones IP al dominio, nombres de máquinas, intercambiadores de correo y servidores de nombres.

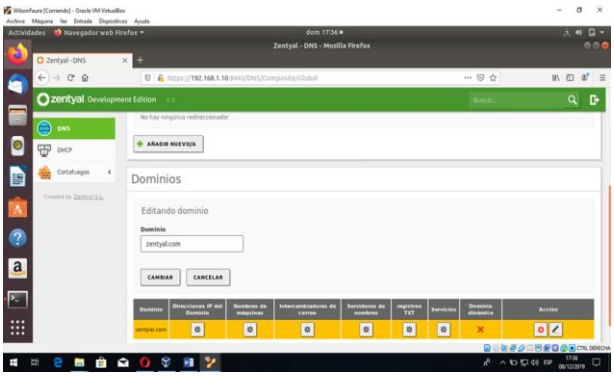


Figura 22. Configuración DNS Server – Fuente propia

Ahora se abre la opción configuración en el módulo DHCP y en la casilla servidor de nombres primario cambiamos la opción “personalizado” por “DNS local de zentyal”, luego se guarda los cambios, como muestra la siguiente figura.

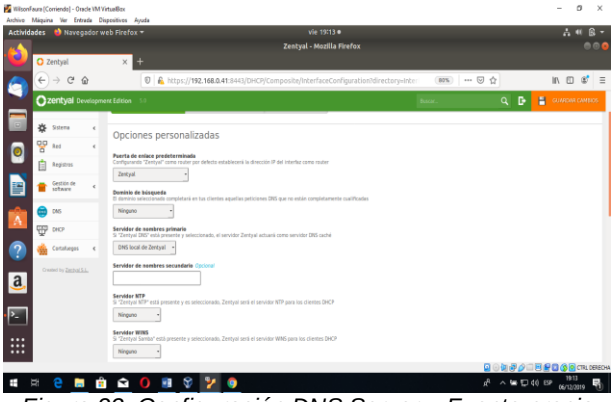


Figura 23. Configuración DNS Server – Fuente propia

Como podemos ver el servicio DNS de Zentyal está funcionando correctamente, pues la dirección DNS predeterminada es la dirección del servidor de zentyal, además si se realiza un ping al dominio recientemente creado “zentyal.com”, resuelve de manera exitosa.

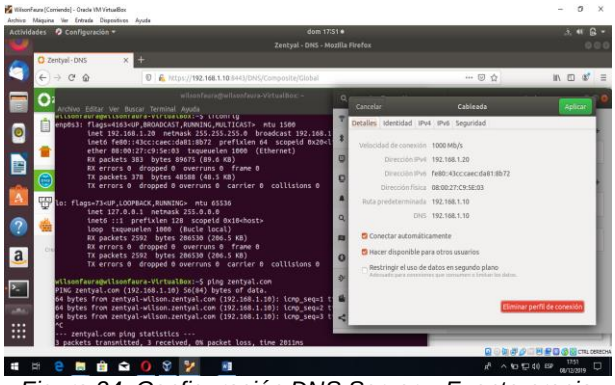


Figura 24. Configuración DNS Server – Fuente propia

3.1.3. CONFIGURACIÓN CONTROLADOR DE DOMINIO

Descargar el módulo, esto lo hacemos desde la interfaz de zentyal, en el menú de la parte izquierda seguimos la ruta gestión de software, componentes de Zentyal, seleccionamos Domain Controller and file Sharing, luego damos clic en instalar.

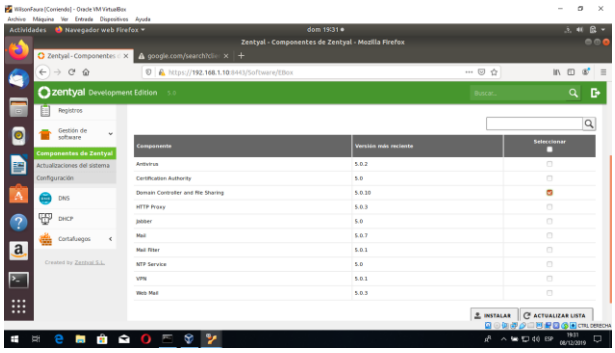


Figura 25. Controlador de dominio – Fuente propia

Ahora aparece en el menú las opciones de usuarios y equipos, dominio y compartición de ficheros, se selecciona dominio, configuración y se puede ver que se encuentra deshabilitado, se deja las opciones por defecto y se guarda.

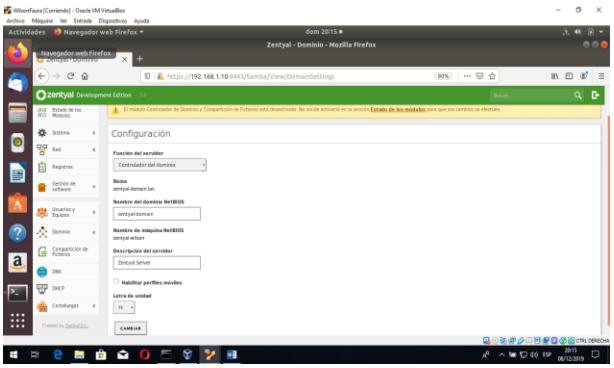


Figura 26. Controlador de dominio – Fuente propia

Regresamos a la página principal, estado de los módulos y se selecciona el check del módulo controlador de dominio, también se debe habilitar los módulos antivirus y NTP que se instalaron en este paso. luego se guarda los cambios y aceptar.

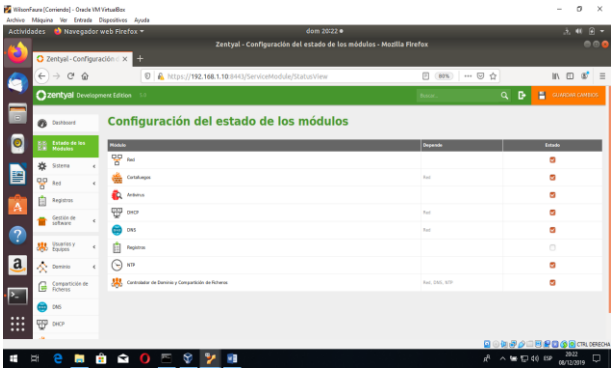


Figura 27. Controlador de dominio – Fuente propia

Se crean los usuarios, se dirige a la opción usuarios y equipos, gestionar y se crea un nuevo usuario, ingresando los datos correspondientes y se da clic en “añadir”, se crean los usuarios necesarios y/o requeridos.

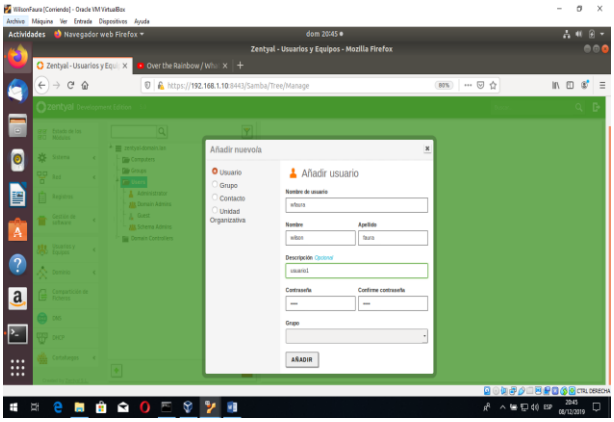


Figura 28. Controlador de dominio – Fuente propia

También se puede crear grupos, yendo a la opción usuarios y equipos, gestionar y se crea un nuevo grupo, ingresando los datos correspondientes y se da clic en “añadir”, por último, se asocia los usuarios al grupo recientemente creado.

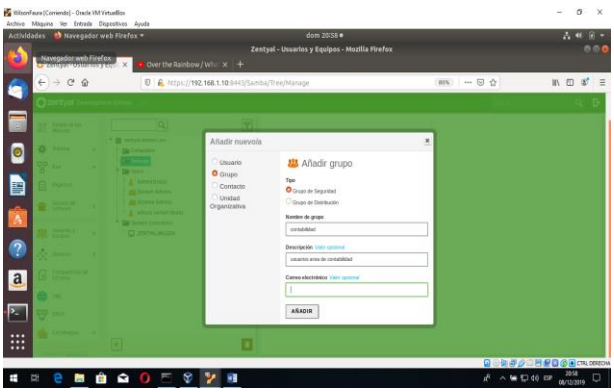


Figura 29. Controlador de dominio – Fuente propia

Para añadir los equipos cliente al dominio se debe descargar un software desde la dirección de github en pantalla, en este caso se descargó la versión para 64 bits deb.sh esta pesa 7,96 MB.

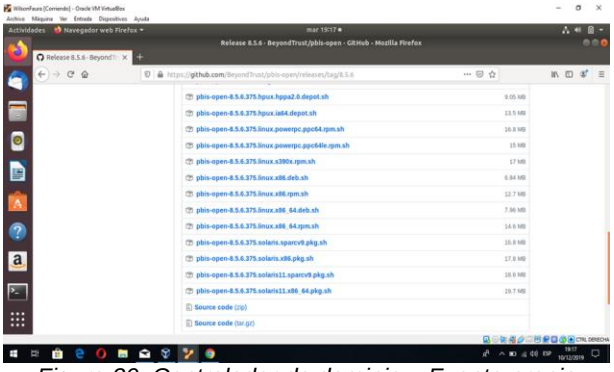


Figura 30. Controlador de dominio – Fuente propia

Ahora se abre una terminal, se loguea como root, se ubica en el escritorio y se lista los archivos, como no está en verde se sabe que no cuenta con el atributo de ejecución, se activa con chmod 777, luego se vuelve a listar y como se nota ya se puede ejecutar.

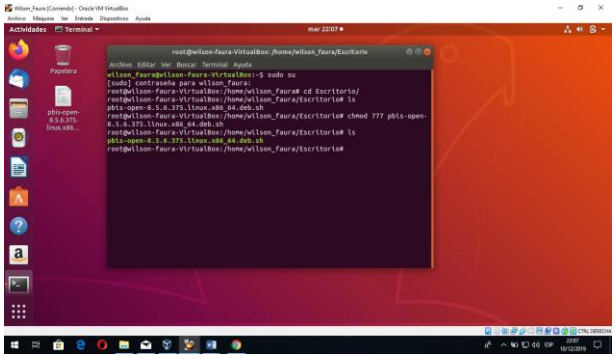


Figura 31. Controlador de dominio – Fuente propia

Ahora se ejecuta ./pbis-open-8.5.6.375.linux.x86_64.deb.sh para descomprimir el archivo y luego se reinicia el sistema con reboot. Ahora se hace un nslookup al equipo dominio para ver que se resuelva correctamente.

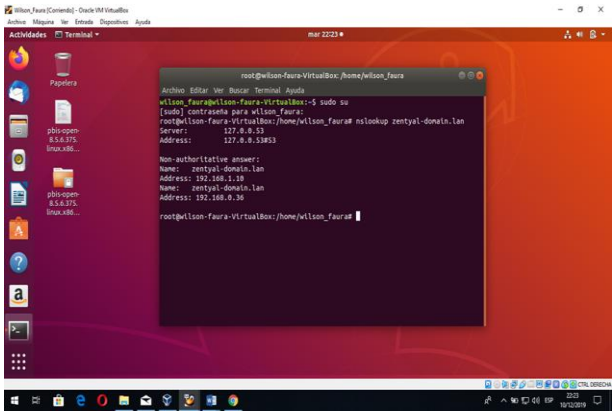


Figura 32. Controlador de dominio – Fuente propia

Ahora se ubica en el directorio opt/pbis/bin, Después se ejecuta la línea para ingresar la máquina al servidor domainjoin-cli join --disable ssh nombreServidor nombreUsuario@nombreServidor

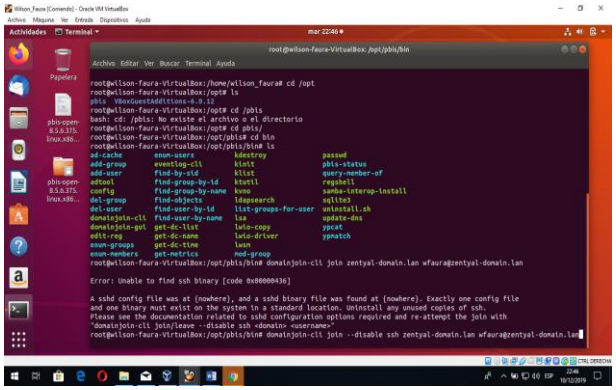


Figura 33. Controlador de dominio – Fuente propia

Por último, se ingresa nuevamente a la terminal como root, se ingresa al fichero con la ruta que aparece en la figura, una vez adentro se modifica según la figura, ahora se ejecuta el siguiente comando /opt/pbis/bin/config LoginShellTemplate /bin/bash para que se use como Shell por defecto el bash.

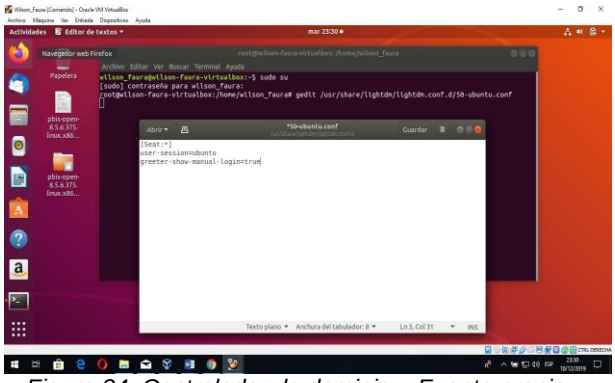


Figura 34. Controlador de dominio – Fuente propia

Una vez se reinicia y cómo se puede ver en esta última figura. ya se tiene el cliente Ubuntu unido al dominio del servidor zentyal y además se está logueado con uno de los usuarios creados en el servidor

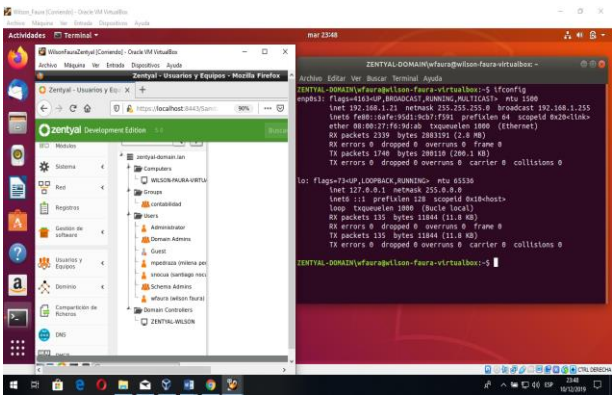


Figura 35. Controlador de dominio – Fuente propia

3.2. TEMÁTICA 2: PROXY NO TRANSPARENTE:

Implementación y configuración detallada del control del acceso de una estación GNU/Linux Ubuntu Desktop a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 3128.

La definición de Prieto R. (2016) Comúnmente un servidor proxy, es un equipo informático que intercepta conexiones de red hechas desde un cliente a un servidor de destino. Por lo tanto, un Proxy transparente en cuanto a su aplicación es transparente para el usuario, en el cuan no resulta necesario agregar los datos del servidor proxy para el uso del servidor proxy.

Por lo tanto, según Enic68 (2011) en un Proxy No Transparente es necesario asignar a cada cliente (computador de usuario) la IP del servidor proxy y el puerto para su uso. De modo que la conexión a este se establecerá una vez configurado en el browser de la máquina cliente la IP y el puerto del servidor por medio del cual se desea navegar (Proxy) siendo esta configuración asignada a la arquitectura de seguridad.

Se da inicio a la implemntación del servicio anteriomente mencionado: Se inicia con la instalación y/o activación de los módulos y/o servicios.

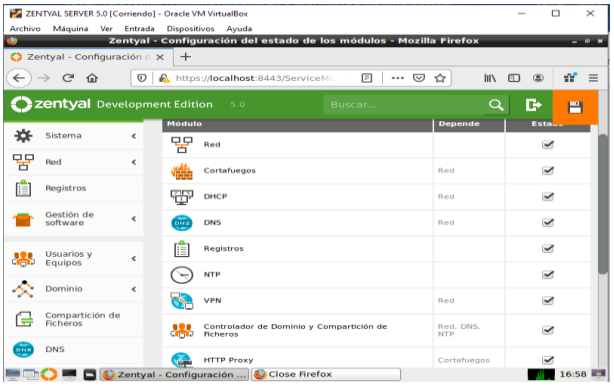


Figura 36. Activación de los módulos requeridos no activados.

Se realiza la configuración de la red.

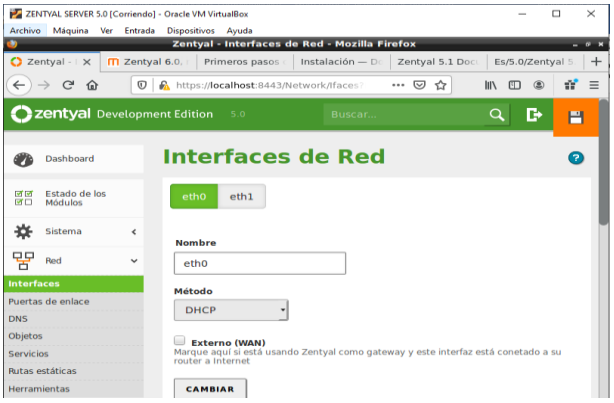


Figura 37. Configuración de la Red WAN DHCP

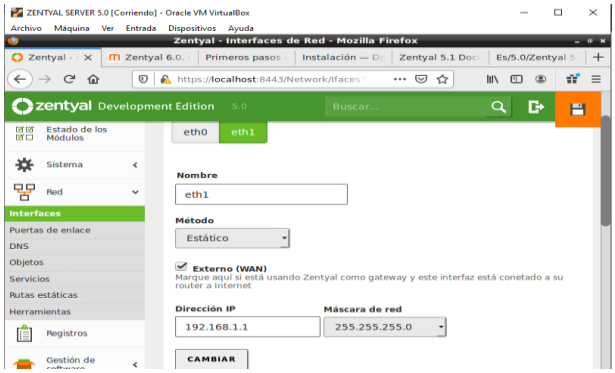


Figura 38. Configuración de la Red LAN Estática.

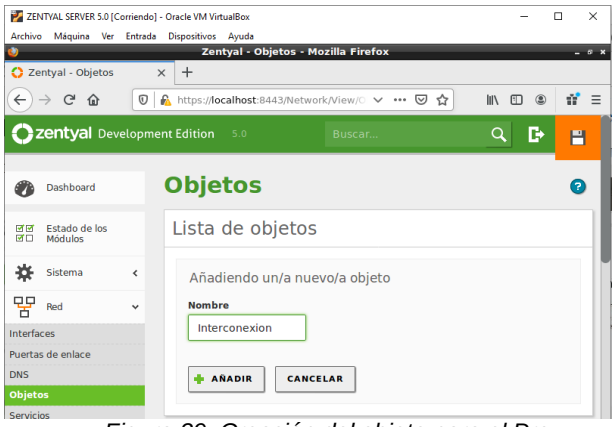


Figura 39. Creación del objeto para el Proxy

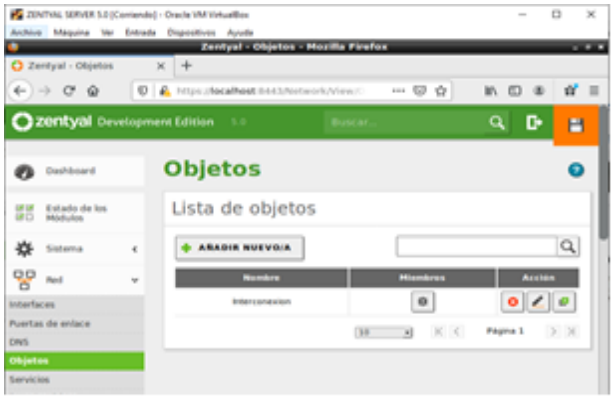


Figura 40. Lista de objetos agregados.

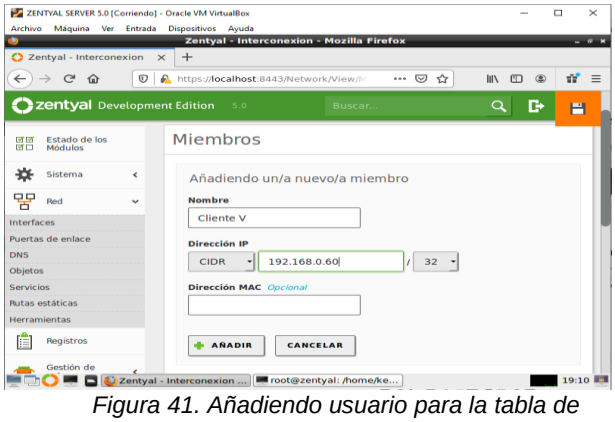


Figura 41. Añadiendo usuario para la tabla de acceso.

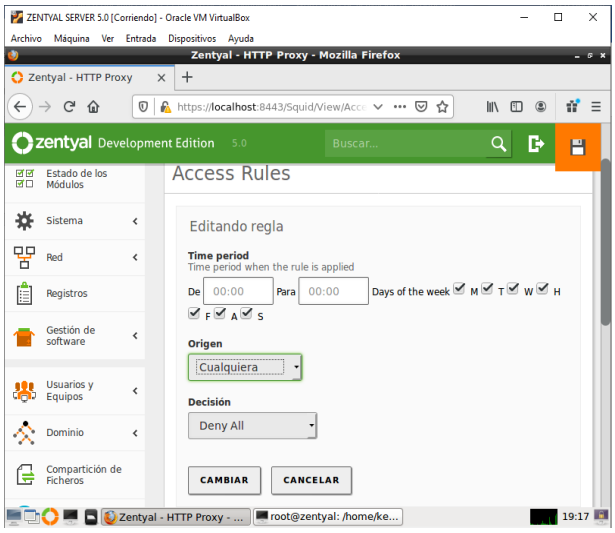


Figura 42. Configuración de Proxy no trasparente.

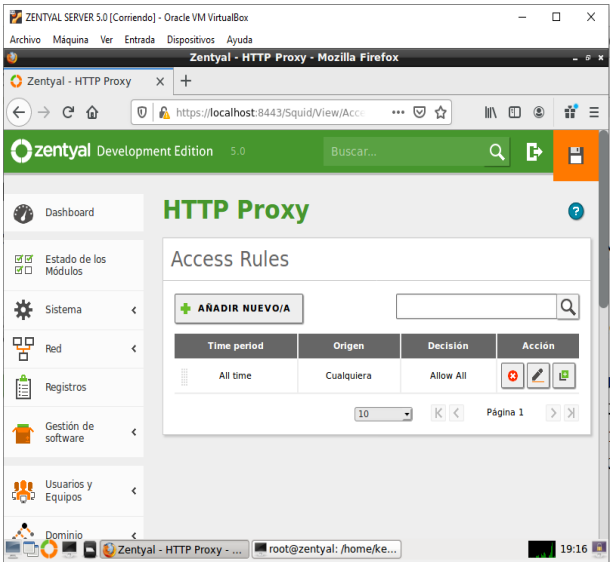


Figura 43. Reglas de acceso en el servicio.

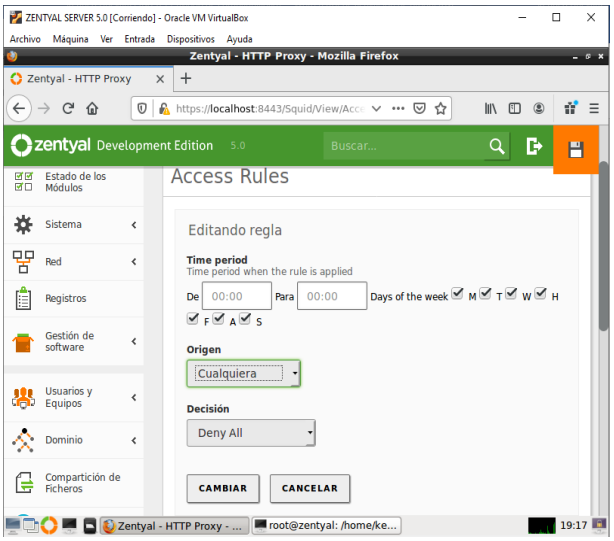


Figura 14. Configuración de la regla de acceso.

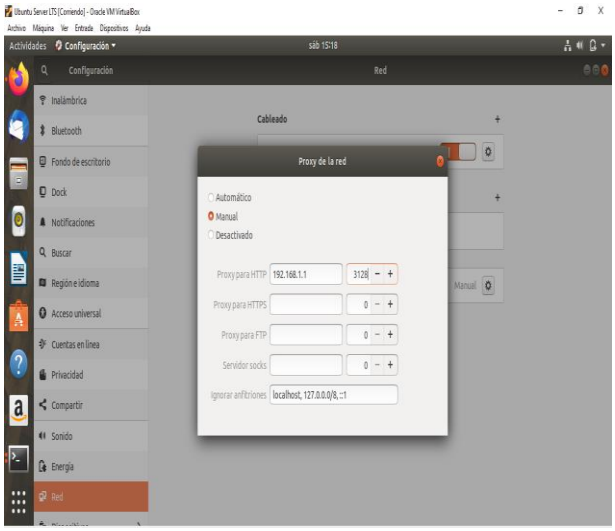


Figura 45. Configuración de la ruta de Proxy.

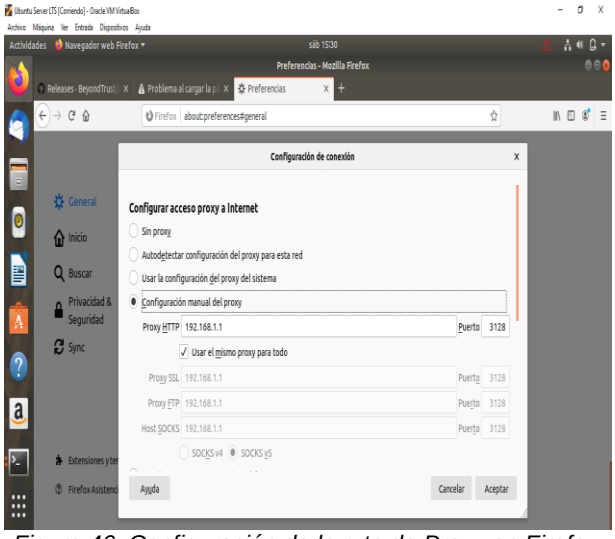


Figura 46. Configuración de la ruta de Proxy en Firefox.

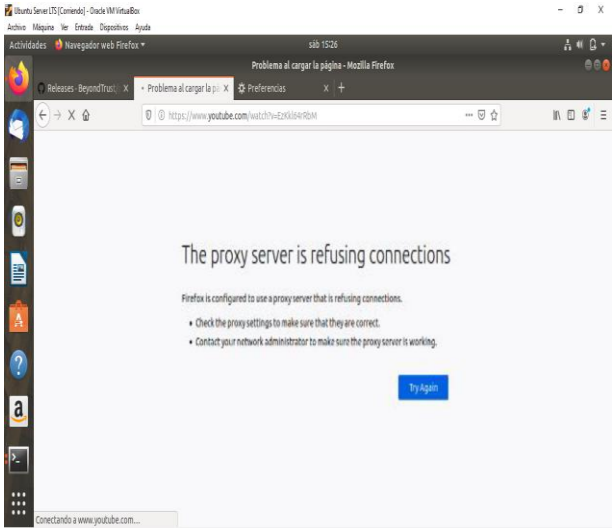


Figura 472. Denegación como resultado de las configuraciones anteriores.

3.3. TEMÁTICA 3: CORTAFUEGOS:

Implementación y configuración detallada para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux Ubuntu Desktop.

Se procede a instalar Firewall (cortafuegos) y DNS server para poder realizar la configuraciones necesarias y requeridas como sigue:

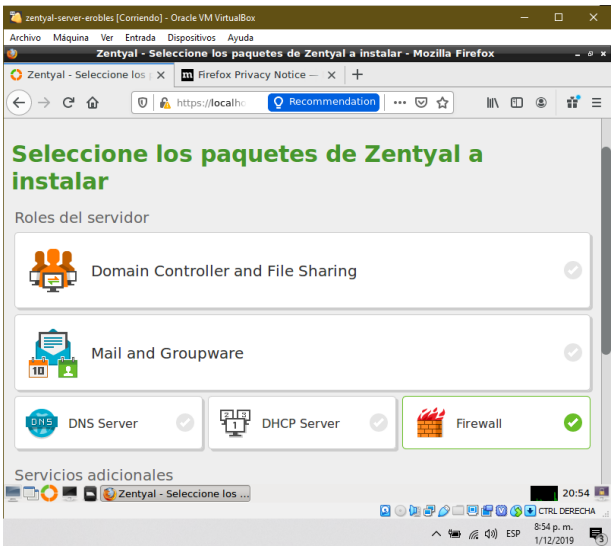


Figura 48 – Instalamos Firewall en el server de Zentyal – Fuente propia.

Se configura la tarjeta para uso del firewall (192.168.10.254)

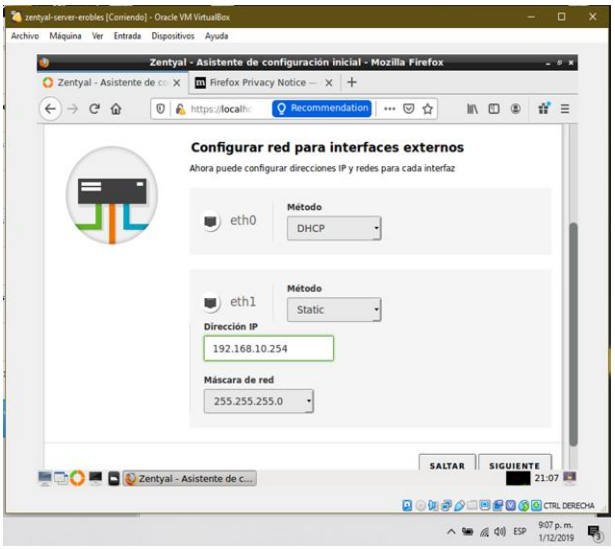


Figura 49 – Configuramos tarjetas en el server Zentyal – Fuente propia.

Se configura la tarjeta red de una estación de trabajo GNU/Linux Ubuntu Desktop a la red que va a ser filtrada por firewall.

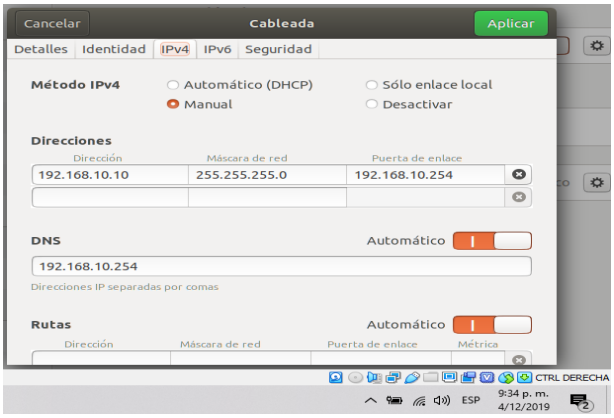


Figura 50 – Configuración tarjeta de red equipo cliente – Fuente propia.

En la siguiente figura se puede observar que el equipo cliente tiene conexión con el Cortafuegos y navegación a internet:

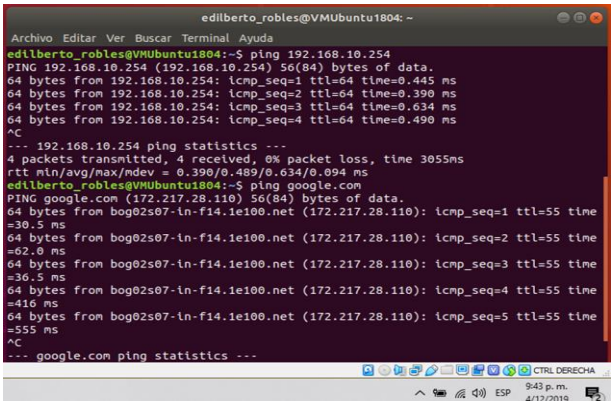


Figura 51 – Conexión al firewall y a internet del equipo cliente – Fuente propia.

Se ingresa a la dashboard y se dirige al Cortafuegos → reglas de filtrado para redes internas → configurar reglas:

Figura 52 – Configuración cortafuegos de Zentyal – Fuente propia

Se procede a configurar las reglas dando clic en “Configurar reglas” y añadir nuevo/a para restringir a los portales Web de entretenimiento y redes sociales como YouTube, Facebook y Spotify.

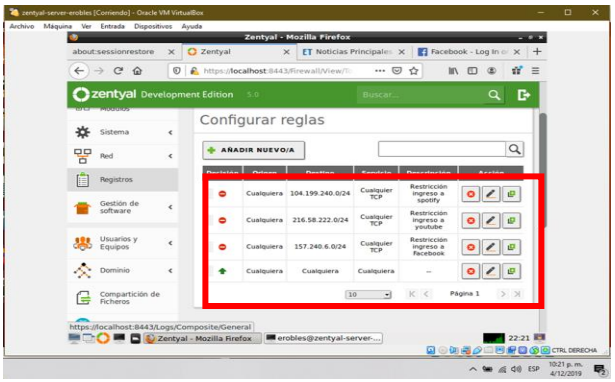


Figura 53 – Configuración de las reglas del cortafuego de Zentyal – Fuente propia.

se procede a guardar los cambios y dirigirse a la maquina Desktop para verificar la aplicabilidad de las reglas:

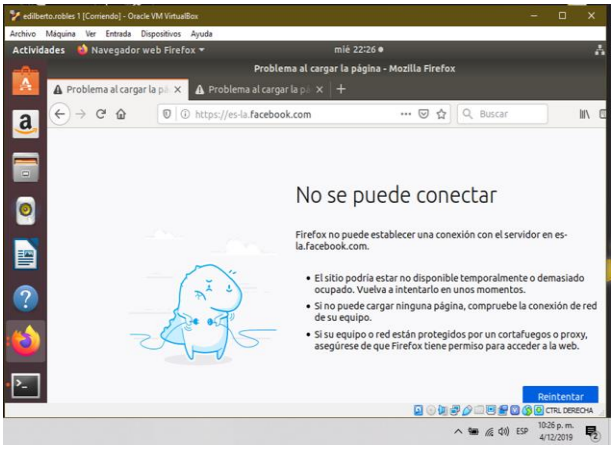


Figura 54 – Denegación del acceso a Facebook por el cortafuegos de Zentyal – Fuente propia.

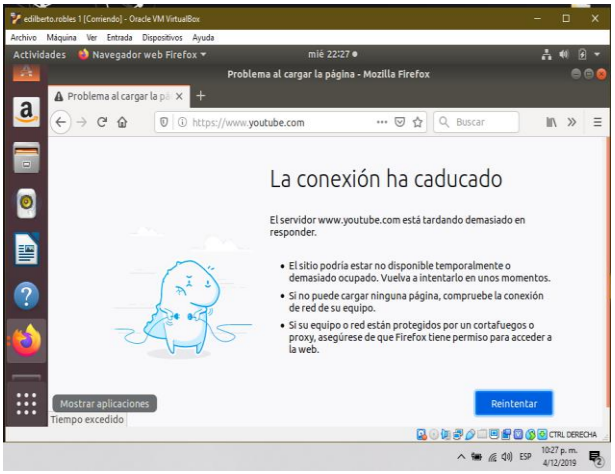


Figura 55 – Denegación del acceso a YouTube por el cortafuegos de Zentyal – Fuente propia

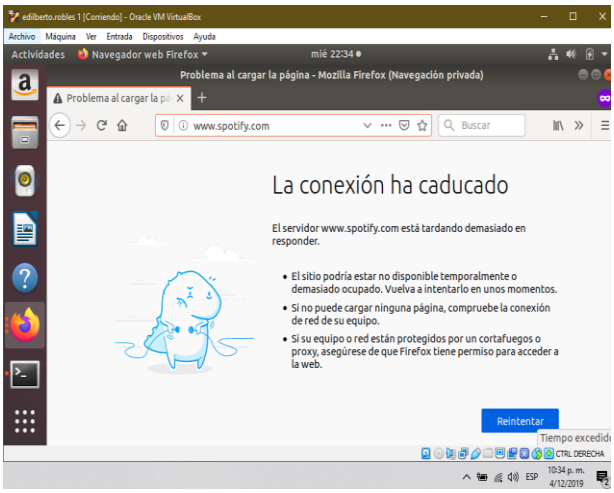


Figura 56 – Denegación del acceso a spotify por el cortafuegos de Zentyal – Fuente propia.

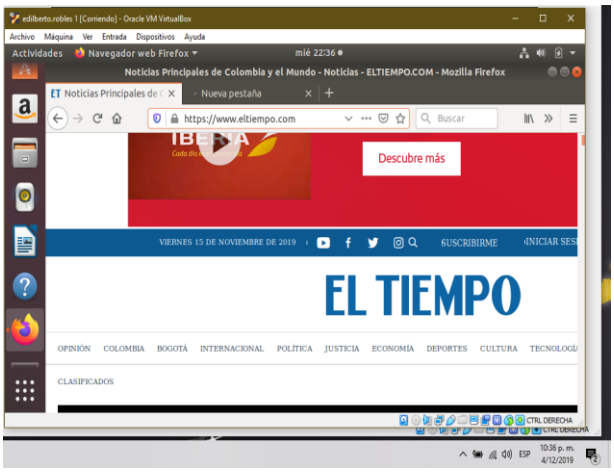


Figura 57 – Acceso a páginas no restringidas por el cortafuegos de Zentyal – Fuente propia.

3.4. TEMÁTICA 4: FILE SERVER Y PRINT SERVER:

Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux Ubuntu Desktop a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras

3.5. TEMÁTICA 5: VPN:

Implementación y configuración detallada de la creación de una VPN que permita establecer un túnel privado de comunicación con una estación de trabajo GNU/Linux Ubuntu Desktop. Se debe evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

PRIMERO SE DEBE REALIZAR LA AUTORIDAD DE CERTIFICACIÓN (CA).

Zentyal integra OpenSSL®, para la gestión de la Autoridad de Certificación y del ciclo de vida de los certificados expedidos por esta.

CONFIGURACIÓN DE UNA AUTORIDAD DE CERTIFICACIÓN CON ZENTYAL

En Zentyal, el módulo Autoridad de Certificación es autogestionado, lo que quiere decir que no necesita ser habilitado en Estado de los Módulos como el resto, sino que para comenzar a utilizar este servicio hay que inicializar la CA. Las funcionalidades del módulo no estarán disponibles hasta que no se haya efectuado esta acción.

se accede a la Autoridad de Certificación ▸ General y se encontrará con el formulario para inicializar la CA. Se requerirá el Nombre de Organización y el número de Días para expirar. Además, también es posible especificar opcionalmente Código del País (acrónimo de dos letras que sigue el estándar ISO-3166-1 [5]), Ciudad y Estado.

Figura 60 – Creación certificado de Zentyal – Fuente propia.

A la hora de establecer la fecha de expiración hay que tener en cuenta que en ese momento se revocarán todos los certificados expedidos por esta CA, provocando la parada de los servicios que dependan de estos certificados.

Una vez que la CA ha sido inicializada, ya se puede expedir certificados. Los datos necesarios son el Nombre Común del certificado y los Días para Expirar. Este último dato está limitado por el hecho de que ningún certificado puede ser válido durante más tiempo que la CA. En el caso de que se esté usando estos certificados para un servicio como podría ser un servidor de correo, el Nombre Común deberá coincidir con el nombre de dominio del servidor. Por ejemplo, si se utiliza el nombre de dominio hq.zentyal.org para acceder al interfaz de administración web de Zentyal, será necesario un certificado con ese Nombre Común. En el caso de que el certificado sea un certificado de usuario, se usa normalmente su dirección de correo como Nombre Común.

Opcionalmente se pueden definir Subject Alternative Names [6] para el certificado. Estos sirven para establecer nombres comunes a un certificado, como una dirección de correo para firmar los mensajes de correo electrónico.

Todo certificado que expida la CA recién creada no será reconocido por software de terceros, como navegadores web o clientes de correo. Esto es debido a que la CA no es oficial, no obstante, a pesar de poder obtener mensajes como el de la siguiente imagen, el tráfico estará cifrado.

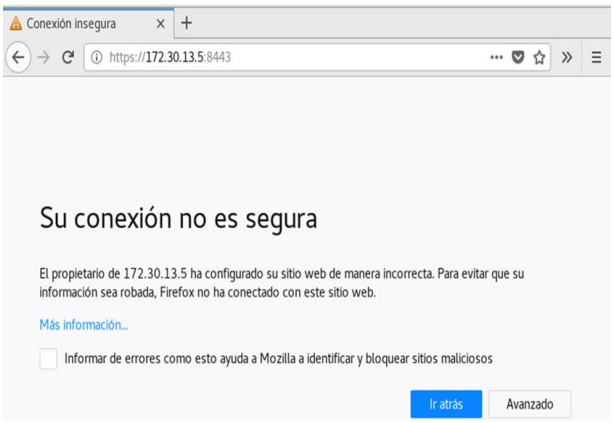


Figura 61 – Creación certificado de Zentyal – Fuente propia.

En Autoridad de Certificación ▸ Certificados de Servicios podemos encontrar la lista de módulos de Zentyal que usan certificados para su funcionamiento. Cada módulo genera sus certificados autofirmados, pero podemos remplazar estos certificados por otros emitidos por nuestra CA.

Para cada servicio se puede generar un certificado especificando su Nombre Común. Si no existe un certificado con el nombre especificado, la Autoridad de Certificación lo creará automáticamente.

Figura 62 –Certificado para servicios de Zentyal –

Fuente propia.

Una vez activado, se debe reiniciar el módulo sobre el que se ha activado el certificado para que lo comience a utilizar, al igual que si renueva el certificado asociado.

Como se ha comentado anteriormente, para la versión segura de varios protocolos (como por ejemplo mail) es importante que el nombre que aparece en el Nombre común del certificado coincida con el nombre que ha solicitado el cliente. Por ejemplo, si el certificado tiene como Nombre común hq.zentyal.org y el cliente teclea mail.hq.zentyal.org, su cliente le mostrará una alerta de seguridad y considerará que el certificado no es válido.

Lista de puntos a comprobar para desplegar un certificado:

- La autoridad de certificación ha sido creada, el módulo del servicio se ha instalado.
- Se ha creado un nombre en el DNS para el servicio (Registro A o CNAME), de tal forma que el cliente lo pueda resolver, por ejemplo 'hq.zentyal.org'.
- Se ha creado un certificado para el servicio específico, por ejemplo, servidor web con un Common Name que coincide con el DNS 'hq.zentyal.org', después de activar el certificado, podremos verlo en Autoridad de Certificación ▸ General.
- Se han configurado los protocolos seguros para el módulo de correo.
- Se ha importado el certificado de la CA (no el certificado del servicio específico) en el sistema o en la aplicación del cliente, por ejemplo, el cliente de correo.
- El usuario configura su cliente de correo apuntando a hq.zentyal.org.
- El usuario es capaz de resolver la DNS a una dirección IP, el Common Name coincide perfectamente con su petición, y el certificado presentado por el servicio está firmado por una autoridad de confianza.
- La aplicación del usuario es capaz de comenzar una sesión segura sin mostrar ningún aviso de seguridad.

Configuración de un servidor OpenVPN con Zentyal

Se puede configurar Zentyal para dar soporte a clientes remotos (conocidos como Road Warriors). Esto es, un servidor Zentyal trabajando como puerta de enlace y como servidor VPN, que tiene varias redes de área local (LAN) detrás, permitiendo a clientes externos (los road warriors) conectarse a dichas redes locales vía servicio VPN.

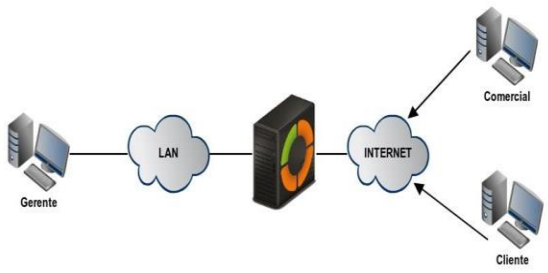


Figura 63 –Mapa de red para Zentyal – Fuente propia.

El objetivo es conectar al servidor de datos con los otros 2 clientes remotos (Comercial y Cliente) y estos últimos entre sí.

Para ello se necesita crear una Autoridad de Certificación y certificados individuales para los dos clientes remotos, que se crea mediante Autoridad de certificación ▸ General. También se necesita un certificado para el servidor VPN, sin embargo, Zentyal expedirá este certificado automáticamente cuando cree un nuevo servidor VPN. En este escenario, Zentyal actúa como una Autoridad de Certificación.

Una vez se tenga los certificados, se debe poner a punto el servidor VPN en Zentyal mediante Crear un nuevo servidor. El único parámetro que se necesita es introducir para crear un servidor es el nombre. Zentyal hace que la tarea de configurar un servidor VPN sea sencilla, ya que establece valores de forma automática.

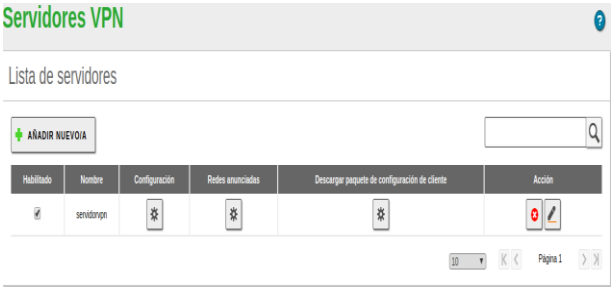


Figura 64 –Añadir servidores en Zentyal – Fuente propia.

Los siguientes parámetros de configuración son añadidos automáticamente, y pueden ser modificados si es necesario: una pareja de puerto/protocolo, un certificado (Zentyal creará uno automáticamente usando el nombre del servidor VPN) y una dirección de red. Las direcciones de la red VPN se asignan tanto al servidor como a los clientes. Si se necesita cambiar la dirección de red se debe asegurar que no entra en conflicto con una red local. Además, se informará automáticamente de las redes locales, es decir, las redes conectadas directamente a los interfaces de red de la máquina, a través de la red privada.

Como se peude ver, el servidor VPN estará escuchando en todas las interfaces externas. Por tanto, se debe poner al menos una de las interfaces propias como externa vía Red ▸ Interfaces. En este escenario sólo se necesitan dos interfaces, una interna para la LAN y otra externa para Internet.

Si se requiere que los clientes de VPN puedan conectarse entre sí usando su dirección de VPN, se debe activar la opción Permitir conexiones entre clientes.

El resto de opciones de configuración se peuden dejar con sus valores por defecto en los casos más habituales.

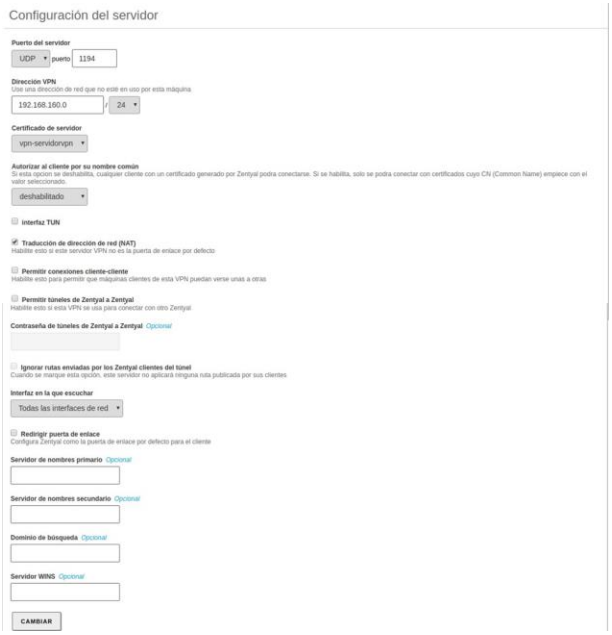


Figura 65 –Configuración servidor VPN – Fuente propia.

Configuración de servidor VPN

En caso de que se necesite una configuración más avanzada: Dirección VPN:

Indica la subred virtual donde se situará el servidor VPN y sus clientes. Se debe tener en cuenta que esta red no se solape con ninguna otra y que a efectos del cortafuegos, es una red interna. Por defecto 192.168.160.1/24, los clientes irán tomando las direcciones .2,*.3*, etc.

Certificado de servidor:

Certificado que mostrará el servidor a sus clientes. La CA de Zentyal expide un certificado por defecto para el servidor, con el nombre vpn-<nuestronombredevpn>. A menos que queramos importar un certificado externo, lo habitual es mantener esta configuración.

Autorizar al cliente por su nombre común:

Requiere que el common name del certificado del cliente empiece por la cadena de caracteres seleccionada para autorizar la conexión.

Interfaz TUN:

Por defecto se usa una interfaz de tipo TAP, más semejante a un bridge de capa 2, podemos usar una interfaz de tipo TUN más semejante a un nodo de IP capa 3.

Traducción de dirección de red (NAT):

Es recomendable tener esta traducción activada si el servidor Zentyal que acepta las conexiones VPN no es la puerta de enlace por defecto de las redes internas a las que podremos acceder desde la VPN. De tal forma que los clientes de estas redes internas respondan al Zentyal de VPN en lugar de a su puerta de enlace. Si el servidor Zentyal es tanto servidor VPN como puerta de enlace (caso más habitual), es indiferente.

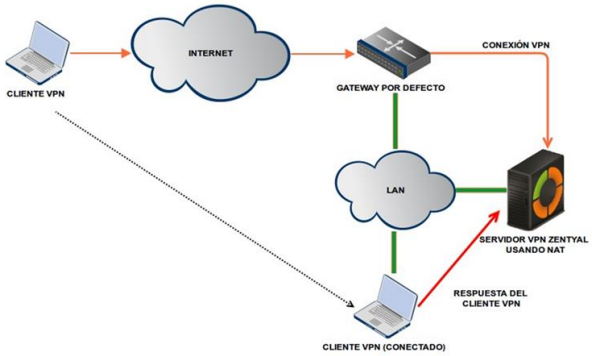


Figura 66 –Servidor VPN usando NAT – Fuente propia.

Servidor VPN usando NAT para convertirse en la puerta de enlace por defecto

Redirigir puerta de enlace:

Si esta opción no está marcada, el cliente externo accederá a través de la VPN a las redes anunciadas, pero usará su conexión local para salir a Internet y/o resto de redes alcanzables. Marcando esta opción podemos conseguir que todo el tráfico del cliente viaje a través de la VPN.

La VPN puede indicar además servidores de nombres, dominio de búsqueda y servidores WINS para sobrescribir los propios del cliente, especialmente útil en caso de que hayamos redirigido la puerta de enlace.

Tras crear el servidor VPN, debemos habilitar el servicio y guardar los cambios. Posteriormente, se debe comprobar en Dashboard que un servidor VPN está funcionando.

Figura 67 –Demonios OpenVPN – Fuente propia.

Widget del servidor VPN

Tras ello, se debe anunciar redes, es decir, establecer rutas entre las redes VPN y otras redes conocidas por nuestro servidor. Dichas redes serán accesibles por los clientes VPN autorizados. Para ello se da de alta objetos que se hayan definido, ver Abstracciones de red de alto nivel en Zentyal, en el caso más habitual, todas nuestras redes internas. Podremos configurar las redes anunciadas para este servidor VPN mediante la interfaz Redes anunciadas.

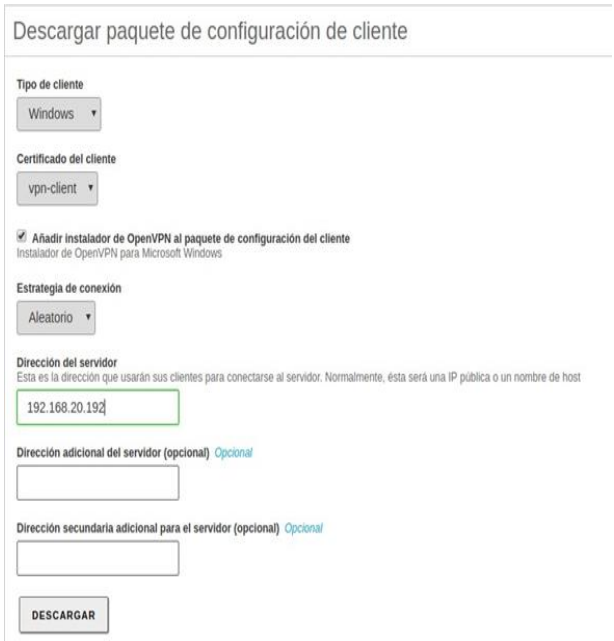
Figura 68 – Lista anunciados servidor VPN – Fuente propia

Redes anunciadas para nuestro servidor VPN

Una vez hecho esto, es momento de configurar los clientes. La forma más sencilla de configurar un cliente VPN es utilizando los bundles de Zentyal, paquetes de instalación que incluyen el archivo de configuración de VPN específico para cada usuario y, opcionalmente, un programa de instalación. Estos están disponibles en la tabla que aparece en VPN ▸ Servidores, pulsando el icono de la columnaDescargar bundle del cliente. Se pueden crear bundles para clientes Windows, Mac OS y Linux. Al crear un bundle se seleccionan aquellos certificados que se van a dar al cliente y se establece la dirección externa del servidor a la cual los clientes VPN se deben conectar.

Como se puede ver en la imagen más abajo, tenemos un servidor VPN principal y hasta dos secundarios, dependiendo de la Estrategia de conexión intentaremos la conexión en orden o probaremos con uno aleatorio.

Además, si el sistema seleccionado es Windows, se puede incluir también un instalador de OpenVPN™. Los bundles de configuración los descargará el administrador de Zentyal para distribuirlos a los clientes de la manera que crea más oportuna.



Descargar paquete de configuración de cliente

Un bundle incluye el fichero de configuración y los ficheros necesarios para comenzar una conexión VPN.

Ahora se tiene acceso al servidor de datos desde los dos clientes remotos. Si se quiere usar el servicio local de DNS de Zentyal a través de la red privada será necesario configurar estos clientes para que usen Zentyal como servidor de nombres. De lo contrario no se podrá acceder a los servicios de las máquinas de la LAN por nombre, sino únicamente por dirección IP. Así mismo, para navegar por los ficheros compartidos desde la VPN [3] se debe permitir explícitamente el tráfico de difusión del servidor Samba.

Los usuarios conectados actualmente al servicio VPN se muestran en el Dashboard de Zentyal. Tendremos que añadir este widget desde Configurar widgets, situado en la parte superior del Dashboard

Widget con clientes conectados

Configuración de un servidor VPN para la interconexión de redes con Zentyal

En este escenario tenemos dos oficinas en diferentes redes que necesitan estar conectadas a través de una red privada. Para hacerlo, se usa Zentyal en ambas como puertas de enlace. Una actuará como cliente VPN y otra como servidor. La siguiente figura ilustra esta situación:

Figura 69 – Descarga de paquetes – Fuente propia

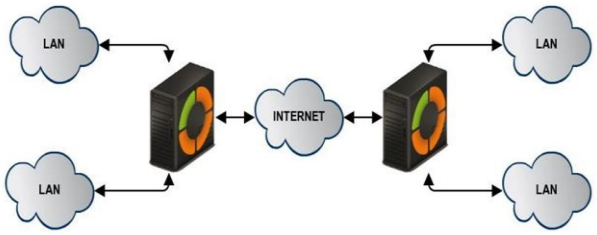


Figura 70 – Interconexión de sedes con zentyal – Fuente propia

Interconexión de sedes con Zentyal mediante túnel VPN

El objetivo es conectar varias sedes, sus servidores Zentyal, así como sus redes internas, de tal forma que podemos crear una infraestructura única para nuestra empresa de forma segura a través de Internet. Para ello, debemos configurar un servidor VPN de forma similar al anterior punto.

Sin embargo, se necesita hacer dos pequeños cambios, habilitar la opción Permitir túneles Zentyal a Zentyal para intercambiar rutas entre servidores Zentyal e introducir una Contraseña de túneles de Zentyal a Zentyal para establecer la conexión en un entorno más seguro entre las dos oficinas. Hay que tener en cuenta que tendremos que anunciar las redes LAN en Redes anunciadas.

Otra diferencia importante es el intercambio de rutas, en el escenario de roadwarrior descrito más arriba, el servidor envía las rutas al cliente. En el escenario de servidor a servidor, las rutas se intercambian en ambos sentidos y se propagan a otros clientes usando el protocolo RIP [4]. Por lo que en los servidores que actúan como clientes VPN del nodo central también es posible añadir las Redes Anunciadas que serán propagadas a los demás nodos.

Figura 70 – Lista de clientes – Fuente propia

Zentyal como cliente de VPN

Para configurar Zentyal como un cliente VPN, se puede hacer a través de VPN ▸ Clientes. Se tiene que darle un nombre al cliente y activar el servicio. Se puede establecer la configuración del cliente manualmente o automáticamente usando el bundle dado por el servidor VPN. Si no se usa el bundle, se tendrá que dar la dirección IP y el par protocolo-puerto donde estará aceptando peticiones el servidor. También será necesaria la contraseña del túnel y los certificados usados por el cliente. Estos certificados deberán haber sido creados por la misma autoridad de certificación que use el servidor.

Figura 71 – Subir paquetes – Fuente propia

Configuración automática del cliente usando el paquete VPN

Cuando se guardan los cambios, en el Dashboard, se puede ver un nuevo demonio OpenVPN™ ejecutándose como cliente con la conexión objetivo dirigida al servidor propio otro servidor Zentyal que actúa como servidor.

Figura 72 – Verificación en demonios OpenVPN –

Fuente propia

4. RESULTADOS

Como resultado podemos observar que la instalación del servicio GNU/Linux que se llevó a cabo se concretó correctamente y el acceso denegado a internet por medio del proxy no transparente también fue exitoso al ser probado en la otra máquina como cliente.

Por otra parte, se puede observar que mediante el uso del cortafuegos de Zentyal, se puede controlar el acceso o no de los diferentes sitios web entre otros, de igual manera se puede denegar o no los diferentes tipos de servicios, el cual permite administrar de forma correcta y controlada la infraestructura de TI de una manera óptima.

5. DISCUCIONES

Se puede deducir que, para resolver diferentes problemáticas de infraestructura de red, como las de migración de sistemas operativos, de servicios y de la puesta en marcha de sistemas de seguridad, se da con la implementación de servicios de gestión de infraestructura IT de mayor nivel para Intranet y Extranet en las compañías y/o instituciones complejas, con el uso de plataformas GNU/LINUX Zentyal server como sistema operativo.

Llevando a cabo la instalación, configuración e implementación de servicios de gestión de infraestructura TI, como son: DHCP server, DNS server, controlador de dominio, proxy no transparente, cortafuegos, file server, print server, VPN, de donde se puede interactuar, administrar y/o gestionar todos los servicios necesarios para una red de TI, para sí realizar una ejecución y parametrización de todos los servicios bajo plataformas GNU/LINUX y su validación de la aplicabilidad de toda una infraestructura tecnológica robusta, compleja y de alta calidad para las entidades y/o empresas, garantizando la confidencialidad, integridad y disponibilidad de la información de una manera optima y controlada.

6. CONCLUSIONES

- Se realizó investigación sobre un entorno de trabajo y se dio solución a unas necesidades específicas con GNU/Linux bajo Zentyal Server, para así realizar la implementación de todo lo que abarca con los servicios de gestión de infraestructura IT: DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server y Print Server, File Server y Print Server.
- Por medio de la práctica se buscó comprender y abordar el OS Zentyal 5.0 y probar su funcionamiento en cuanto a un servidor no transparente.
- Se logro instalar el servicio GNU/Linux Zentyal 5.0 y a su vez se logró configurar adecuadamente para configurar el proxy no transparente. Alexander Ramírez (27 de junio de 2018). Instalación y configuración de ZENTYAL. [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=VgOv2pcUfxU
- Se realizó la implementación de servicios de infraestructura IT de mayor nivel para Intranet y Extranet en instituciones complejas, aplicando y Wikipedia (2019) ISO 3166-1. Recuperado de https://es.wikipedia.org/wiki/ISO_3166-1afianzando conocimientos de este, en base de la resolución de un planteamiento y contextualización del problema cotidiano de la vida real.
- Zentyal server, es un servidor liviano, sencillo de instalar y fácil de configurar, ofrece al administrador de la red varias posibilidades gráficas para instalar diferentes servicios que funcionan de manera correcta como DHCP o DNS.
- El acceso al Dominio creado en Zentyal server, requiere de una configuración previa del sistema operativo Ubuntu, en donde se hace necesario instalar los módulos de controlador de dominio, el cual permite la adición del equipo al dominio de Zentyal.
- La instalación y configuración del Zentyal Server es muy sencilla e intuitiva, cumple con el propósito para el cual fue diseñado el cual es cumplir con las necesidades de una empresa, solo se debe prestar atención al momento de configurar las tarjetas de red ya que de estas depende el buen funcionamiento del sistema.

7. REFERENCIAS

[1]. Prieto, R, *"Cómo configurar proxy SQUID en modo transparente"*. May 2016. Recuperado de: https://www.raulprietofernandez.net/blog/gnu-linux/como-configurar-proxy-squid-en-modo-transparente

[2]. Enic68," Proxy *transparente o no?"*. JUN 2011. Recuperado de: https://forum.netgate.com/topic/34808/proxy-transparente-o-no

[3]. Zentyal, *"La interfaz web de administración de Zentyal"*. Recuperado de: https://doc.zentyal.org/es/firststeps.html

[4]. Zentyal, *"Documentación de Zentyal 5.1"*. Recuperado de: https://doc.zentyal.org/5.1/es/installation.html#configuracion-inicial

[5]. Villada, R. J. L. (2015). Instalación y configuración del software de servidor web (UF1271). (Páginas. 121 – 148). Madrid, ES: IC Editorial. Recuperado de https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=4310544&ppg=126

[6]. Molina, R. F. J., & Polo, O. E. (2014). Servicios en red. (Páginas. 105 - 481). Recuperado de https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3229687&ppg=104

[7]. Wikipedia (2019) Zentyal. Recuperado de https://es.wikipedia.org/wiki/Zentyal

[8]. Manuel Cabrera Caballero (8 de Abril de 2018). Zentyal Server | Instalación y primeros pasos DETALLADOS para ti. [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=tG_NHAUYUbU
[9]. OpenSSL. (2019). Welcome to OpenSSL! Recuperado de: https://www.openssl.org/
[10]. Hedrick, C (1988). Protocolo de información de enrutamiento. Recuperado de https://www.ietf.org/rfc/rfc1058